APPENDIX 1A

BNFL INC. OVERALL SAFETY APPROACH

This page intentionally left blank.

APPENDIX 1A – BNFL INC. OVERALL SAFETY APPROACH

CONTENTS

FIGURES

APPENDIX 1A – BNFL INC. OVERALL SAFETY APPROACH

TABLES

APPENDIX 1A – BNFL INC. OVERALL SAFETY APPROACH

1.0 INTRODUCTION

BNFL Inc.'s overall approach to safety ensures that workers (including both facility and co-located workers) and the public are adequately protected during all aspects of the Tank Waste Remediation System-Privatization (TWRS-P) Facility operation. This includes both normal and off-normal operations and accident conditions.

The principal aspects of our approach are founded on the proven, successful experience of the BNFL team members in both the UK and the United States. Furthermore, the British Nuclear Fuels plc policy for uniform adherence to corporate safety principles and practices underlies the BNFL Inc. safety and design practices and is the basis for our approach.

The approach follows a sequence as the design evolves, with each succeeding step building on the previous steps. In addition, the approach is graded (i.e., tailored) to the nature of the identified hazards and hazardous situations. The approach relies on both engineered features and administrative controls to ensure adequate safety. This appendix primarily addresses the engineered features. Administrative controls (procedures and training) addressed in Section 1.3 of the *Integrated Safety Management Plan* (ISMP) and Section 3.4 of the *Initial Safety Analysis Report* (ISAR).

BNFL's overall safety approach is summarized in Chapter 2.0. Specific aspects of the approach are discussed in more detail in Chapters 3.0 through 7.0. Chapter 8.0 contains a demonstration of the application of the safety approach using the high-level waste (HLW) receipt tanks as an example.

It should be noted that this ISAR appendix describes a process that is different in some aspects from the information contained within the main body of the ISAR. These differences have arisen from changes to the BNFL safety approach as a result of discussions with the DOE Regulatory Unit (RU). The differences occur primarily in the areas of design classification, application of design requirements to safety equipment, identification of items important-to-safety, and assignment of quality levels.

APPENDIX 1A – BNFL INC. OVERALL SAFETY APPROACH

2.0 SAFETY APPROACH AND METHODOLOGIES

BNFL Inc.'s safety approach is founded on the premise that the facility design must demonstrate adequate safety, conform to the top-level principles, and comply with applicable laws and regulations. To achieve this, safety items are identified through a number of processes. These include the following:

- Facility Design Description (Identification of Work)
- Hazard Identification and Control
- Defense-in-Depth Evaluation
- Identification of Safety Design Class systems, structures, and components (SSC)
- Identification of items Important-to-Safety
- Confirmation that the Risk from Accidents is Acceptable

Figure 2-1 is a schematic representation of the BNFL Inc. safety approach showing the principal steps. It should be noted that this approach is iterative, with numerous feedback reassessment loops to address process and regulatory changes as well as design evolution. For clarity of presentation, these loops are not shown in Figure 2-1.

The following subsections provide a summary description of our methodologies.

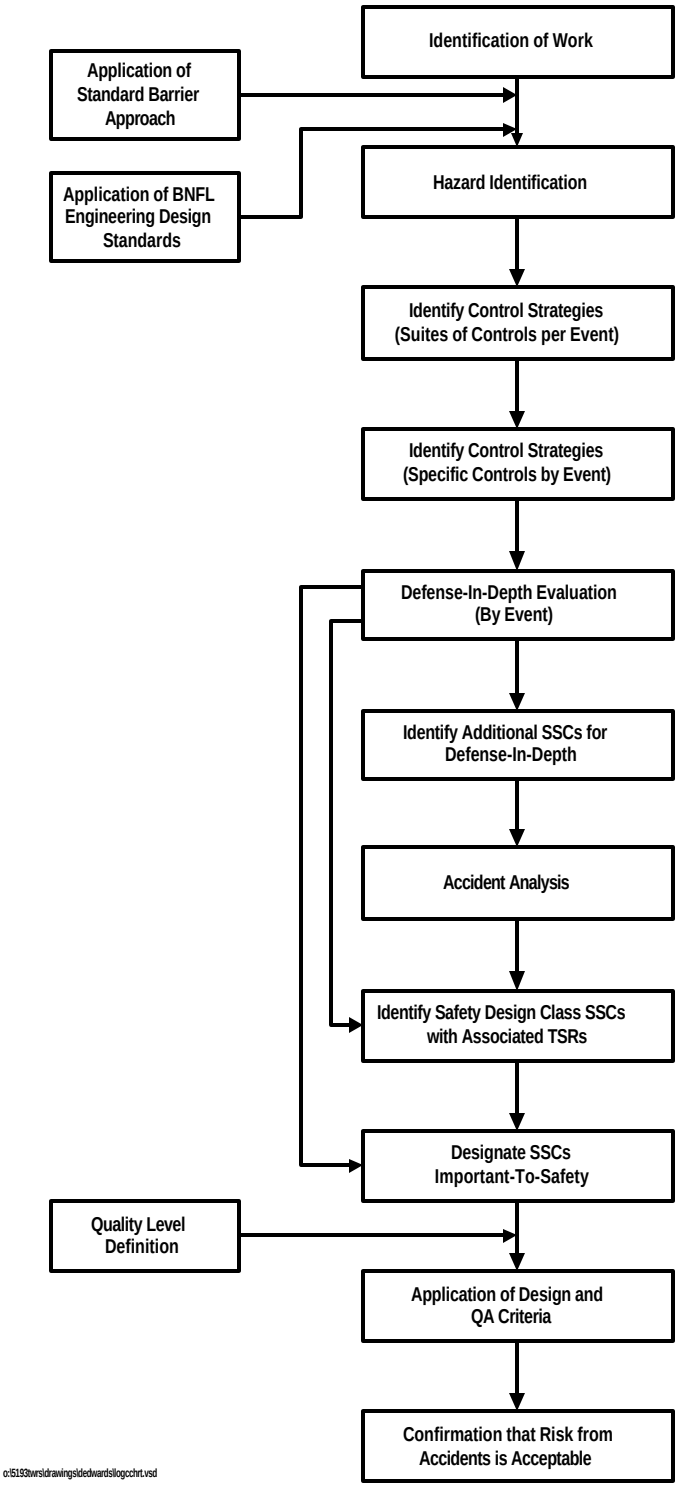
2.1 FACILITY DESIGN DESCRIPTION

The BNFL waste treatment facility (LAW-Only and combined HLW/LAW) is designed to treat mixed waste from the Hanford site underground storage tanks. In designing the waste treatment facility and support buildings, BNFL has recognized and incorporated design features necessary to prevent and mitigate the hazards associated with the wastes and hazardous chemicals used in the waste treatment process and with the associated energetic systems (e.g., steam, electrical distribution). The process BNFL used to identify potential hazards is described in the *Hazards Analysis Report* (HAR) (BNFL-5193-HAR-01, 1997). Features incorporated into the facility design to prevent and mitigate hazards are described in BNFL's ISAR (BNFL-5193-ISAR-01 1998).

The waste treatment facility comprises concrete cells that serve as confinement barriers and provide personnel radiation protection. Inside these concrete cells, the mixed waste is contained within high-intensity stainless-steel vessels, piping, and equipment. The concrete cells are partially lined with stainless steel and include sumps to provide control for spills or leaks, in accordance with the requirements of *Washington Administrative Code* (WAC), "State Dangerous Waste Regulations", Chapter 173-303-640. The materials of construction for the vessels, piping, equipment, and the cell liners have been selected to be fully compatible with the chemicals and mixed waste to be treated in the process cell. Vessel and equipment data sheets have been prepared and are on file that identify the appropriate materials of construction. Facility drawings identify materials to be used for piping and cell liners.

APPENDIX 1A – BNFL INC. OVERALL SAFETY APPROACH

Figure 2-1. Overall Safety Approach Flowchart.



APPENDIX 1A – BNFL INC. OVERALL SAFETY APPROACH

Personnel radiation shielding assessments that determined the sizing of the concrete cell walls have been prepared and are on file. These shielding assessments also have been used to determine maintenance requirements for process equipment. As a general design philosophy, BNFL selects process equipment that does not require maintenance, such as fluidic pumps and valves. Where this approach is not practicable, BNFL locates high-maintenance components of process equipment (e.g., pump and agitator motors) in accessible areas, that include integral design features for personnel radiation and hazards protection. For example, the agitator motor for each of the LAW melter feed preparation vessels (V3320, V3322, V3324) is located exterior to the vitrification process cell. The agitator shaft passes through a shielded penetration and connects to the agitator and motor.

In some cases, process equipment must be located within process cells to provide the necessary personnel protection. To enhance the safe operation of the facility, equipment located within process cells is designed to be maintained remotely. For example, ultrafilter units may require replacement of the filter elements during operations. The ultrafilter unit is designed for remote removal of the top of the ultrafilter housing and replacement of the ultrafilter element. The ultrafilter units are positioned at the top of the pretreatment process cell. A removable shield plug is incorporated in the process cell roof above each ultrafilter element. A shielded flask device is positioned atop the removable shield plug and the plug removed. The shielded flask device provides confinement and radiation protection for personnel during the replacement of the ultrafilter element. The ultrafilter element is withdrawn from the housing into the shielded flask, the shield plug re-installed, and the flask removed to a station where the ultrafilter is packaged for disposal. A new ultrafilter element is installed in a similar manner.

BNFL has also incorporated into the design of the waste treatment facility features to protect the worker and the environment from chemical spills and leaks. For the treatment of tank waste, BNFL has selected chemical reagents that pose the lowest hazards possible. To minimize the residual hazards associated with the chemical reagents used for treatment of the tank waste, BNFL has designed the chemical reagent vessels located within the waste treatment facility to contain the minimum amount of chemical solutions needed for a 24-hour operating period (the calculations are on file) to limit the potential chemical exposure to workers. Additionally, BNFL has incorporated spill confinement for the chemical reagent vessels located outside the waste treatment facility.

BNFL also recognizes the hazards associated with energetic systems such as electrical power distribution, compressed air generation and distribution, and steam generation and distribution. BNFL's design of these systems in Part A of the TWRS-P contract is not as detailed as that of the waste treatment facility. However, BNFL will apply nationally-accepted design codes and standards (e.g., National Fire Protection Agency, Institute of Electrical and Electronics Engineers [IEEE], National Electrical Manufacturers Association, Occupational Safety and Health Administrative) to ensure protection from hazards. System description documents have been prepared and are on file that incorporate appropriate nationally-recognized design codes and standards as a design basis for support systems (e.g., bulk chemical storage, steam, air, water, electricity) associated with the waste treatment facility.

2.2 HAZARD IDENTIFICATION AND CONTROL

BNFL Inc. selected a team of experts to develop the basis of design for the treatment of the tank waste. The team was composed of experts in design engineering and operations at similar facilities, safety analysis, formulation, chemistry, vitrification of glass products, and risk assessment

APPENDIX 1A – BNFL INC. OVERALL SAFETY APPROACH

and management. Throughout the process, the team composition was enhanced as needed to address specific topics.

Based on their combined knowledge, this team developed the treatment process and facility design described in the *Technical Report*. Their background at similar facilities enabled them to identify design features and hazards inherent with the treatment processes developed. Many of these features are the same engineering design safety principles that support the safe operation of other BNFL facilities. The HAR documents the process and hazards evaluated.

The team identified the hazards and controls to ensure safety at the TWRS-P Facility. The team addressed hazards and hazardous situations at all levels from minor accidents to those events that can have significant consequences, both onsite and offsite. This level of safety is inherent in BNFL nuclear chemical facility design and results from the experience-based understanding of the approaches needed to ensure adequate protection.

Once the treatment process was defined and the associated hazards and hazardous situations identified, the same team of experts identified control strategies through three “pathways”, as described in the following paragraphs.

First, a standard confinement barrier approach was applied throughout the conceptual design. This approach requires that, when highly radioactive or hazardous materials are present, a minimum of three confinement barriers generally are specified. These confinement barriers consist of: (1) the vessels and piping containing the material and the vessel ventilation system, (2) the cell that contains the vessel (and piping) and the ventilation system serving the cell, and (3) the operating corridor outside the cell with its ventilation system. The TWRS-P Facility design currently reflects this multiple confinement barrier philosophy.

Second, the vessels and equipment making up the process are specified with safety features and controls according to the established nuclear design standards used successfully by BNFL in the design of their nuclear chemical processing facilities at Sellafield and elsewhere in the UK. This includes such things as high-level and high-high-level tank alarms, corrosion allowances, and redundant fans. As with the confinement barriers, these features are also standard (i.e., not event-specific). They have been developed over many years based on prudent engineering practices and as safety features required to protect against hazards similar to – and more severe than – those postulated at TWRS-P. Depending on the current level of design evolution, many of these features already have been incorporated into the TWRS-P design as part of the standard design approach used by BNFL.

Third, the Process Hazards Analysis identifies the specific hazards and hazardous situations associated with the TWRS-P process, and then identifies the hazards control strategies to prevent or mitigate the consequences of the postulated events. As described in ISMP Section 1.3.4 and ISAR Section 4.6.1, this is a formalized, documented, and iterative process performed by the teams of highly experienced individuals to produce a design in full compliance with the applicable laws and regulations and in conformance with the DOE stipulated top-level standards and principles. Because the TWRS-P Facility is in the pre-conceptual design stage, control strategies have not been specified on a one-to-one basis for every hazardous situation. Instead, suites of potential controls have been listed in the HAR. As the design evolves, specific controls will be identified through the performance of detailed hazard and operability study (HAZOP) analyses.

APPENDIX 1A – BNFL INC. OVERALL SAFETY APPROACH

There are design features providing controls to protect workers and the public, even though event-specific controls have not been identified for every hazardous situation identified in the HAR. In fact, as discussed previously, the current design incorporates a considerable number of controls that arise from the standard application of the multiple confinement barrier approach and the further application of BNFL nuclear design standards. In many cases, these standard control strategies effectively prevent or mitigate the hazardous situations identified in the HAR.

As the design progresses and the necessary design detail becomes available, event-specific controls will be identified where necessary, and these controls will be incorporated into the facility design to supplement the standard controls. The final result will be a design that effectively addresses identified hazardous situations, provides multiple barriers against releases of material or exposure to workers and the public, and uses experienced-based, proven design approaches to account for contingencies and unexpected conditions.

Chapter 3.0 describes specific topics associated with the hazard identification and control process.

2.3 DEFENSE-IN-DEPTH EVALUATION

Defense-in-depth is a governing principle in the design of all BNFL nuclear facilities. Defense-in-depth ensures that multiple barriers protect individuals during normal operations and from the consequences of accidents involving radioactive or hazardous material.

When considering overall facility safety, it is important to note that the TWRS-P features that BNFL specifies as part of the defense-in-depth process are in addition to those specified as part of the hazard identification and control process discussed in the preceding section. Therefore, defense-in-depth items provide, in essence, a second level of safety overlaying those needed to prevent or mitigate accidents. As a result, defense-in-depth evaluations generally occur when the design has evolved to the point that specific hazard control schemes have been specified.

BNFL uses a formalized process in its approach to defense-in-depth. For significant and potentially significant accidents, the existing barriers against material release or personnel exposure are identified. These barriers then are evaluated to address the following considerations:

- Independence and diversity (can a single initiating event fail some or all)
- The potential for consequential damage to multiple barriers (domino effect)
- Robustness against the expected challenges to their function
- Interaction with operators and the contribution of operators to defense-in-depth

For severe hazards, the application of defense-in-depth increases accordingly. Therefore, as it is determined that more protection – or more diverse protection – is required, additional barriers are specified. This determination is based on a number of criteria including the potential consequences of the event (high potential consequences would lead to more protection), the number and nature of existing barriers, experience with similar hazards at similar nuclear facilities, and variability of the potential consequences to workers or the public.

Furthermore, as discussed in Section 2.6, BNFL Inc. will perform risk analyses to confirm that facility accident risk goals are met. These risk analyses may show that certain events are significant contributors to the overall accident risk. Additional defense-in-depth items will be specified to reduce that risk.

APPENDIX 1A – BNFL INC. OVERALL SAFETY APPROACH

Chapter 4.0 describes specific topics associated with the defense-in-depth process.

2.4 IDENTIFICATION OF SAFETY DESIGN CLASS ITEMS

As a part of ensuring an adequate level of safety for workers and the public, the TWRS-P Facility design also must ensure that the consequences of accidents are prevented or mitigated such that the applicable exposure standards are not exceeded under credible conditions. For TWRS-P, the accident exposure standards are given in Table A of the BNFL document entitled *Radiological Exposure Standards for Workers Under Accident Conditions* (RESW). This table, which is repeated in SRD Section 2.0 and ISAR Table 4-27, is derived from, and in conformance with, the top-level exposure standards contained in Table 1 of DOE/RL-96-0006.

Although accidents that have the potential to exceed the exposure standards are highly unlikely, their potential consequences are sufficiently severe such that the function of prevention or mitigation features must be ensured. Consequently, BNFL has established a design classification system to provide that added assurance to DOE. In this system, SSCs needed to ensure that public and worker accident exposure standards are not exceeded are designated Safety Design Class. Enhanced levels of design, quality assurance, and operational requirements are applied to Safety Design Class items. The design classification process establishes a third, independent provision of safety that reinforces the protection provided by the other two processes previously described.

Performance of accident analyses that show the potential for limits to be exceeded is the “usual” method for designating items Safety Design Class. However, items are also designated Safety Design Class independent of a specific accident analysis. These are items that protect the facility worker from potentially serious events. Typically, they present a challenge to the facility worker severe enough that mitigation is prudent, regardless of the result of the consequence analysis. These items typically arise from the HAR, and are identified as part of defense-in-depth. Such items are listed in ISAR Tables 4-46 and 4-47.

Chapter 5.0 describes specific topics associated with the Safety Design Class identification process.

2.5 IDENTIFICATION OF ITEMS IMPORTANT-TO-SAFETY

The design classification process described in the preceding section provides high visibility and a high level of requirements to those SSCs needed to prevent or mitigate accidents that could exceed exposure standards. It is recognized, however, that there are many other items that contribute to the overall safety of the facility. These items are identified as safety features in the BNFL process of designating items Important-to-Safety.

Items Important-to-Safety are a subset of the safety items identified in the other processes previously discussed. Specifically, they fall into two groups and include the following:

- SSCs needed to prevent or mitigate accidents that could exceed worker or public radiological and chemical exposure standards and SSCs needed to prevent criticality. This set of SSCs includes front line and support systems needed to meet these exposure standards. This set of Important-to-Safety SSCs is further designated as Safety Design Class

APPENDIX 1A – BNFL INC. OVERALL SAFETY APPROACH

- SSCs needed to achieve compliance with the radiological or chemical exposure standards for the workers and public during normal operation and SSCs that place frequent demands on, or adversely affect the function of Safety Design Class SSCs if they fail or malfunction.

The first group of items falls directly out of the design classification process. The second group can arise in several ways: (1) SSCs identified as significant contributors to safety by the risk analyses that confirm the facility accident risk goals are met, (2) SSCs that are clearly needed to ensure standards for normal operation are not exceeded, (3) SSCs (e.g., bulk shield walls or radiation monitors) that are needed to ensure occupational exposure goals are achieved, (4) SSCs selected based on the dictates of nuclear facility experience and prudent engineering practices, and (5) SSCs whose failure could prevent Safety Design Class SSCs from performing their safety function (e.g., seismic II/I items).

Because the TWRS-P Facility design is in the conceptual phase, the only important-to-safety items identified are those designated Safety Design Class. As the design matures, additional SSCs of the second group will be identified.

Chapter 6.0 describes specific topics associated with the designation of SSCs Important-to-Safety.

2.6 CONFIRMATION THAT THE RISK FROM ACCIDENTS IS ACCEPTABLE

The top-level standards contained in DOE/RL-96-0006 include accident risk goals. BNFL Inc. has committed to meeting these goals and will perform risk analyses as needed to confirm that the goals have been met. These risk analyses will be best estimate analyses based on realistic input and modeling assumptions. In performing these analyses, SSCs capable of preventing or mitigating events will be considered. Estimates of system and component availabilities and reliabilities will consider failure to start and failure to run as well as maintenance-caused unavailabilities.

This risk evaluation process may identify additional preventative and mitigative items that should be added to the design to meet the accident risk goals. Such items would represent an additional level of safety.

2.7 OVERALL SAFETY HIERARCHY

As described previously, the BNFL Inc. overall safety approach uses multiple processes to create a facility design with a safety hierarchy consisting of up to four separate and independent levels of protection that both complement and reinforce each other. These four levels are as follows.

- At the first (baseline) level, the hazard identification and control process implements control strategies that are sufficient in themselves to prevent or mitigate hazardous situations.
- Next, the defense-in-depth process ensures that the control strategies identified provide sufficient diversity. If not, additional levels of protection are specified.
- Third, for the severest accidents (i.e., those that have the potential to challenge accident exposure standards), the design classification process ensures that items that prevent or mitigate these accidents will be capable of performing their specified safety function.
- Finally, to ensure that risks (not just consequences) are properly considered, the risk analysis process identifies other SSCs that need to be incorporated to ensure that accident risk goals are satisfied.

APPENDIX 1A – BNFL INC. OVERALL SAFETY APPROACH

APPENDIX 1A – BNFL INC. OVERALL SAFETY APPROACH

3.0 HAZARD IDENTIFICATION AND CONTROL TOPICS

The design submitted with the Part A contract deliverables has progressed to the point that allowed preparation of process flow diagrams, general layout drawings, and a major plant item list. This design is sufficient to allow the preparation of the cost estimate to support Part B of the contract.

The most important interaction between design and safety at this point in the project is the designation of Safety Design Class SSCs. During Part B, BNFL Inc. will continue the design through four stages of Engineering Flow Diagrams (EFD) as shown in Table 3-1 and two stages of civil structural design (CSD) as shown in Table 3-2. From these two design media, BNFL Inc. will develop additional design media such as vessel data, mechanical data sheets, ventilation flow diagrams, and building layouts. These tables show the various stages of design and the information provided at each stage.

Each stage of the EFDs provides a basis for the next stage of design. In addition, the Stage A EFDs provide information to allow initiation of CSD1 and the Stage B EFDs provide information to allow initiation of CSD2. To support the start of construction, both the Stage B EFDs and CSD2 need to be completed. The EFDs are finalized at the completion of the HAZOP studies that in turn provide the basis for the pre-operational design.

3.1 HAZARD CONTROL STRATEGY DEVELOPMENT

The first hazard evaluation was conducted during preparation of the *Standards Approval Package* (SAP). The level of detail available for this initial review was limited. The design evolved during the performance of the hazard analysis and following the completion of this analysis. In the early stage of this review, conservative assumptions about the hazard of the facility were made that were removed at later stages of the hazard analysis. In addition, certain systems have been removed or changed so that the original hazards identified no longer exist (e.g., replacement of Reillex HPQ resin with SuperLig 639[1]).

The HAR, supporting the conceptual design, has identified the major hazards within that design. During the systematic, team-based hazard identification exercise, qualitative judgements were made by the team of design experts as to the acceptability of hazards within the facility processes. Where hazards were considered unacceptable, team members were asked to remove them as part of design development. This process was conducted by assigning actions to carry the request through to the design process. This reflects the strategy of ensuring that, as far as possible, hazard control is deterministic.

Table 3-1. Engineering Flow Diagram Information

Engineering Flow Diagram	Purpose	Information Available
Stage A	To allow preliminary plant layout development.	Position of main plant items vertically to scale. Correctly identify main equipment and sizes. Add main and process supply pipe work. Number and size of main pipe work.

[1] ™ SuperLig 639 is a trademark of IBC.

APPENDIX 1A – BNFL INC. OVERALL SAFETY APPROACH

Stage B	To allow detailed plant layout development.	Position of main plant items vertically to scale. Correctly identify and size main equipment. Add further pipe work. Number all pipe work. Through wall pipe elevations added (gravity feeds). Valve details added. Control valves identified. All major inline components added. Pipe end connection added. Instrument preliminary details added. Indicate battery limits. Tabulate all miscellaneous equipment (ejectors).
Stage C	To approve plant control and initiate HAZOP studies.	Valve control details confirmed. All instrument details. Operational control loops confirmed and trip/interlocks added.
Stage D	For continuation of HAZOP studies.	Add minor equipment. Indicate modules and wall boxes. Control sequence number (e.g., UX, ZX boxes). Add various EFD drawing conventions. Add Engineering Protective Systems for safety.

The HAR Fault Schedules take each identified hazard and, together with major initiating events, identify the control strategies that could be chosen to control the hazard. At this stage of the project, only major hazards have been identified together with a representative sample of contributing initiating events. This is consistent with the *American Institute of Chemical Engineers* (AIChE) guidelines (AIChE 1992) for hazard identification studies on conceptual designs.

In selecting the hazards for assessment, the safety analysts examined all of the hazards identified and considered their severity with respect to unmitigated consequences. As a result, hazards considered negligible (in terms of either risk or consequence) were not carried over for assessment. This does not mean that they have been forgotten; the Part A HAR is to be used as the basis for the further, more developed hazard assessments to be performed as the design matures during Part B. The hazards rated as negligible for the Part A design will be reassessed during Part B. The accidents with the greatest consequences are summarized in the HAR Chapter 4.0.

APPENDIX 1A – BNFL INC. OVERALL SAFETY APPROACH

Table 3-2. Civil Structural Information

Civil Structural Information	Purpose	Information Needs
CSD1	Used by the structural technical section to carry out the global structural analysis of the building.	Building size. Approximate location of all structural (load bearing) walls (locations of partition walls are not important). Minimum required radiation-shielding thickness for walls and floors. Approximate location of all major (heavy) equipment. Not-to-Exceed weights of all major equipment (heavy equipment). Locations and sizes of all major wall and floor openings.
CSD2	Used by all disciplines to produce the working design calculation, General Arrangements, Reinforcement Concrete, and Architectural and Civil drawings for construction purposes.	Final locations of all structural (load bearing) walls. Final locations of all partition walls. Final locations of all equipment (both major and minor). Final weights of all equipment (both major and minor). Locations and sizes of all wall and floor openings (both major and minor). Locations and sizes of all wall and floor embedments (e.g., wall boxes, floor boxes, equipment anchor bolts, and embedded plates for commodity supports, etc.).

The link between the hazards identified in the Fault Schedule and those carried forward to the ISAR is discussed in ISAR Section 4.6.2.2. Based on the HAR, the safety analysts selected 54 accident scenarios for which a set of bounding analyses were performed to identify Safety Design Class SSCs. These accidents were selected based on their unmitigated release potential. The accidents were grouped into eight categories based on the type of accident (e.g., fire, over pressurization).

The accident from each group with the largest potential for release was analyzed for its consequences. The consequences were compared to the accident exposure standards for the co-located worker and the public. If the calculated consequences exceeded the allowable

APPENDIX 1A – BNFL INC. OVERALL SAFETY APPROACH

exposure standard, a set of mitigating features selected from the control strategies identified in the HAR were designated to control the consequences of the accident.

For each hazard carried over into the ISAR for further evaluation, the control strategy, based on hazard severity, is applied in a general manner. Because all of the initiating events for identified hazards have not yet been identified, a complete, comprehensive control strategy has not yet been specified.

The following is true for each hazard in the ISAR.

1. The quantitative or qualitative estimate of its frequency and consequence is stated, establishing the hazard severity.
2. In the HAR Fault Schedules, protection is specified and defined against identified hazards. This comprises the element of defense-in-depth applicable to accident conditions. In many cases, this protection is the diverse barriers integral to the design. This protection comprises (by definition) additional protection, and traditionally would be characterized as items Important-to-Safety.
3. From the accident analysis in the ISAR, those hazards that have the potential for challenging facility worker, co-located worker, or public exposure standards are identified. From the control strategies, specified in number 2 above, the subset of SSCs designated Safety Design Class are selected. The safety function of each Safety Design Class SSC is clearly defined. Additionally, those elements of the supporting systems (if information is available) required for the component to perform its designated safety function are identified.

The identification of protection, first to incorporate defense-in-depth and second to designate Safety Design Class SSCs, is carried out in a qualitative manner, appropriate for the stage of the Part A design. The process demonstrates that there is a defined method of control against each hazard. When specific details about a control strategy are not available the process ensures that the information is developed during hazard identification and control assessments performed as the design matures during Part B.

In addition to this analysis, safety analysts chose a suite of SSCs to be designated for the protection of the facility worker. As the design progresses, additional features will be identified and the specific Safety Design Class component identified.

The control strategies identified for the hazards in HAR Chapter 6 and the ISAR are shown in Table 3-3.

Part B Activities

In Part B, as the design develops and more detailed information becomes available, the fault schedules, the result of further hazard identification studies, become more detailed. For each hazard, initiating events are identified and protection assigned to each of them. The BNFL design guide, NF 0124, “Operational and Engineered Protective Measures”, is used to bin hazards according to their severity. From the results of this binning, the protection requirements against each initiating event are identified. The degree of protection required is commensurate with the severity of the hazard, that is, there is more need for defense-in-depth against severe hazards than against lesser or minor hazards.

APPENDIX 1A – BNFL INC. OVERALL SAFETY APPROACH

This page intentionally left blank.

APPENDIX 1A – BNFL INC. OVERALL SAFETY APPROACH

Table 3-3. Identified Hazards and Part A Controls.

Number	ISAR Event Number	System Identifier	System Identifier Number	System	Event Description	Part A Control	Comment
1	3	1	8	Entrained Solids Removal	Potential for spray leak	Buried doubly contained lines.	
2		2100	9	LAW Feed Evaporator	Backflow of steam to tank causing high temperature/pressure	Negligible hazard consequence within process recovery parameters.	
3	13	9101	10	LAW Container Decontamination	Degradation of cell HEPA due to moisture	Pre-dryers in offgas plenum.	
4	15	0	10	Double Shell Tank Filling	Loss of HEPA filter because of HEPA filter fire	Analysis showed event not to be credible.	
5	27	1	11	Entrained Solids Removal	Generation of radiolytic gases; buildup in ultrafilter and lines	Analysis showed event not to be credible.	Vessel vent provided
6	33	2200	11	Cs Removal Using Ion Exchange	Hydrogen fire in column	Analysis showed event not to be credible.	Vessel vent provided
7	43	2200	11	Cs Removal Using Ion Exchange	Overpressurization of column from heat generated by caustic/acid mixing or resin degradation	Acid and caustic supplied from separate sources.	
8	25	2200	12	Cs Removal Using Ion Exchange	Ignition of hydrogen evolved by radiolytic decomposition, or degradation of resin	Frequent resin changes.	
9	42	2200	13	Cs Removal Using Ion Exchange	Overpressurization of column from resin degradation or resin discharge line blockage	Frequent resin changes.	
10		9101	13	LAW Product Handling	Worker injury from pipe whip or exposure to high pressure water.	Package unit in cell in decontamination cabinet.	
11	27	1	18	Entrained Solids Removal	Generation of radiolytic gases; buildup in ultrafilter and lines	Analysis showed event not to be credible.	Vessel vent provided
12	1	0	26	Double Shell Tank Filling	Seismic damage to transfer line	Buried doubly contained lines.	
13		3200	114	LAW/HLW Glass melter	Potential for contact with toxic glass forming materials. Work health detriment.	Best Industrial Practice for pneumatic transfer system.	
14		3200	116	LAW/HLW Glass melter	Worker exposed to fire because of ignition of flammable glass forming materials	Reducing agents not allow in process unless concern removed.	
15	2	1614664	117	Tc Removal Using Ion Exchange	Pipe or vessel rupture	Analysis showed event not to be credible.	
16	23	1614664	117	Tc Removal Using Ion Exchange	Fire/explosion because of radiolytic hydrogen production	Analysis showed event not to be credible.	
17	40	1614664	118	Tc Removal Using Ion Exchange	Pressurization from hydrogen (degradation of resin) or steam produced by heat from mixing caustic and acid	Analysis showed event not to be credible.	Vessel vent provided
18	4	1614662	119	Cs Recovery as a Solid	Overflow of V2401 to vessel vent system	Controlled by interlock.	Standard control feature design detail not yet available.
19	19	1614667	119	Cs and Tc Nitric Acid Recovery	Fire in cell (ignition source present)	Fire load minimized in cell.	
20	29	1614661	120	LAW Melter Feed Evaporator	Combustion of ammonia, pump motor ignition source	Analysis showed event not to be credible.	
21	39	1614664	120	Tc Removal Using Ion Exchange	Explosion in vessels (ion exchange columns) due to breakthrough of steam	System designed to cope with steam breakthrough.	
22	41	1614667	120	Cs and Tc Nitric Acid Recovery	Overpressurization of evaporator from heat generated by acid water reaction or radiolytic hydrogen production	Vessel vent system.	
23		1614668	120	HLW Container Decontamination	Worker injury from pipe whip or exposure to high pressure water.	Package unit in cell in decontamination cabinet.	
24	38	1614662	121	Cs Recovery as a Solid	Pressurization of canister from water in canister; steam or radiolytic gases	Analyze offgas for water content.	
25	28	1614661	122	LAW Melter Feed Evaporator	Fire or explosion from radiolytic hydrogen and/or ammonia in feed	Condensers tied to vessel vent system.	
26	30	1614666	122	HLW Melter Feed Receipt and Pretreatment	Radiolytic hydrogen fire/explosion; pump motor ignition source	Analysis showed event not to be credible.	Vessel vent provided
27	14	1614666	129	HLW Melter Feed and Pretreatment	Loss of cooling, boiling of HLW vessel	Long time to boiling.	Backup cooling water system provided.
28		1614688	129	Outcell Process Reagents	Operator exposure to hazardous chemicals because of adverse chemical reaction from mixing incompatible reagents.	Tanks separated and vent.	Chemicals analyzed before use.
29		3200	130	LAW/HLW Glass melter	Potential for contact with toxic glass forming materials. Worker health detriment.	Design changed no manual handling of glass formers.	
30		1614662	130	Boiler Water Heat Recovery System	Spillage or leakage of very hot water. Potential for worker injury.	System removed from design.	Similar hazards controlled by material specification.
31	51	1614667	131	Cs and Tc Nitric Acid Recovery	Damage to nitric acid stock tanks	Nitric acid tanks located in code designed enclosure.	
32		1614683	133	Outcell Process Reagents	Operator injury, due to reaction (highly exothermic reaction from water addition to acid).	Controlled by interlock.	Standard control feature design detail not yet available.
33		1614667	135	Cs and Tc Nitric Acid Recovery	Potential for contact with concentrated nitric acid.	Addition of safety showers.	
34	10	1614662	136	Cs Recovery as a Solid	Drop and breach of a Cs product canister	All movements in cell.	
35		1614772	139	LAW Vitrification Line Product Handling	Operator exposure to inert filler material or high-pressure fluid systems.	Inert filling material used (sand).	Operations occur in cell.
36		3200	140	LAW/HLW Glass melter	Worker injury from electrical fire or pump motor fire.	Fire load minimized in cell.	
37	11	1614772	142	LAW Vitrification Line Product Handling	Breach of pour seal and release of melter atmosphere	Control on fabrication of pour seal.	
38		1614772	143	Vitrification Product Line	Worker egress may be blocked.	Adequate egress provided from occupied space.	
39	44	1614772	145	LAW Vitrification Line Product Handling	Use of wrong filling material	Single source of filler material.	Operations occur in cell.
40	8	1614667	153	Cs and Tc Nitric Acid Recovery	Enhanced radioactivity to the vent system from loss of cooling	Vessel vent system designed accommodate nitric acid fumes.	
41		1614669	156	Cs and Tc Fresh Resin Addition	Potential for contact with toxic materials. Health detriment resulting from contact with spilled resins or reagents.	Resin receiving system located in code designed structure.	
42		1614669	158	Cs and Tc Fresh Resin Addition	Exposure to toxic fumes resulting from a resin fire or chemical reaction between resin and nitric acid.	Resin and nitric acid stored in segregated areas.	
43	6	3200	160	LAW/HLW Glass Melter	Failure of melter feed line	Melters located in cell.	
44	48	3200	161	LAW/HLW Glass Melter	Overfilling of melter	Canisters sealed against discharge chamber.	
45	7	3200	165	LAW/HLW Glass Melter	Loss of HEPA filtration because of saturation of filter by steam	Pre-dryers in offgas plenum.	
46		1614772	166	LAW Vitrification Line Product Handling	Operator exposure to radioactive materials because of containment from gas buildup inside the container.	Minimize fire loading in cell.	
47	37	3200	167	HLW/LAW Melter	Overpressurization of melter vessel	Standby offgas system sized to handle overpressurization.	
48	35	1614687	171	LAW Vitrification Emergency Offgas System	Breach of line because of pressure caused by chemical reaction in melter	Standby offgas system sized to handle overpressurization.	
49		1614669	174	Cs/Tc Fresh Resin Addition	Resin handling operations can lead to falls an lifting injuries	Resin added mechanically.	
50	47	3200	179	LAW/HLW Glass Melter	Loss of glass containment from corrosion	Refractory material will be selected to limit corrosion.	Testing part of Part B.
51	20	1614687	191	LAW Vitrification Emergency Offgas System	HEPA filter fire	Analysis showed event not to be credible.	

APPENDIX 1A – BNFL INC. OVERALL SAFETY APPROACH

Table 3-3. Identified Hazards and Part A Controls.

Number	ISAR Event Number	System Identifier	System Identifier Number	System	Event Description	Part A Control	Comment
52	26	3200	192	LAW/HLW Glass Melter	Ignition of hydrogen or carbon monoxide evolved in offgas	Offgas system quench removes hazard.	
53	9	3200	193	LAW/HLW Glass melter	Contamination spread through cell	Standby offgas system sized to handle overpressurization.	Ensure no blockage occurs.
54	36	3200	193	LAW/HLW Glass Melter	Failure of emergency offgas to relieve pressure	Standby offgas system sized to handle overpressurization.	Ensure no blockage occurs.
55	5	3200	220	LAW/HLW Glass Melter	Overfilling or leaking of in-cell vessels	Fluidic pump used to transfer solutions.	
56	46	1614672	224	LAW Vitrification Offgas Treatment	Pressurization of melter; potential for loss of glass containment/involuntary glass discharge	HEME change over on high pressure drop.	
57	32	1614672	238	LAW Vitrification Offgas Treatment	Ammonia fire; fan motor is ignition source, oil for burner is additional fuel	SCR separated from fans and located in isolated zone.	
58	34	1614672	239	LAW Vitrification Offgas Treatment	Ammonium nitrate formation because of loss of process parameters (temperature control) and subsequent explosion	SCR operates in temperature range to prevent fires.	Additional up and down stream protection.
59	49	3200	246	LAW/HLW Glass Melter	Catastrophic failure in primary containment via melter refractory penetrations, thermocouple guide tube failure	Thermocouple design prevents occurrence of failure.	Thermocouple tube doesn't breach cell confinement.
60	22	3200	248	LAW/HLW Glass Melter	Fire in melter cell	Analysis showed event not to be credible.	
61	50	3200	248	LAW/HLW Glass Melter	Glass spillage	Canisters sealed against discharge chamber.	
62		3200	265	LAW/HLW Glass melter	Contamination because of dropped components during removal or replacement of melter and/or components.	Maintenance occurs in cell with feeds turned off.	Protective covers for busses and windows.
63		1614776	271	Waste Store Operations	Potential for increased radioactive exposure to workers (debris left in flask).	Flask monitor before use.	
64		1614776	275	Waste Store Operations	Worker exposure to fire (Diesel fuel fire).	Design changed no diesel in area.	
65	45	1614774	285	LAW/HLW Melter Maintenance	Failure of melter due to seismic event	No significant consequence from melter.	Cell contains glass spill.
66		1614776	287	Waste Store Operations	Exposure to hazardous materials.	Shipping cask designed to minimize possibility.	
67	16	1614673	288	HLW Vitrification Offgas Treatment	HEPA filter fire	Analysis showed event not to be credible.	
68	24	1614673	288	HLW Vitrification Offgas Treatment	Ignition of hydrogen/ammonia in process offgas	Analysis showed event not to be credible.	
69		1614776	295	Waste Store Operations	Radiation exposure to operator, gamma gate is open when operator is in the flask introduction area.	Interlock provide to control event.	Standard control feature design detail not yet available.
70		1614776	299	Waste Store Operations	Dropped load/impact hazard	Deign precludes drop of lid.	
71		1614673	304	HLW Vitrification Offgas Treatment	Exposure to radioactive material because of damage to contaminated components resulting from a drop.	Appropriate lifting gear provided.	
72	31	1614671	339	Secondary Offgas Treatment	Hydrogen fire; electrical heater ignition source	Analysis showed event not to be credible.	
73		1614778	343	LAW/HLW Solid Waste Handling	Laser cutting provides a potential of injury to the eye.	Standard safety procedures for laser light.	
74		1614776	344	Waste Store Operations	Potential for increased radioactive exposure to operators (lid not on canister and gamma gate open).	Interlock provide to control event.	Standard control feature design detail not yet available.
75		1614775	385	Cesium Line	High radioactive exposure to worker because of inadvertent posting out of full canister or container.	Interlock provide to control event.	Standard control feature design detail not yet available.
76		1614775	389	Cesium Line	Operator exposure to cesium radiation (gamma door and posting hatch open at the same time).	Interlock provide to control event.	Standard control feature design detail not yet available.
77	52	1614775	399	Cesium Line	Spillage of nitric acid in-cell resulting in evolution of fumes	Interlock provide to control event.	Standard control feature design detail not yet available.
78		1614775	421	Cesium Line	Potential worker contact with nitric acid because of corrosion of pipe work.	Material selection.	
79		1614775	430	Cesium Line	Worker exposure to cesium radiation because of improper cesium loading of the canister.	Amount of CST in each column limit to 90% of allowable.	
80	18	1614775	438	Cesium Line	Fire initiated by plasma welding	Use system from Sellafield.	Shroud weld head.
81		1614775	439	Cesium Line	Airborne radioactive materials because of canister rupture from over pressurization by radiolytic gases (not properly dried)	Moisture monitored in exit gas.	
82	12	1614775	486	Cesium Line	Loss of cell atmosphere control	HVAC system design with appropriate differential and air flows.	
83	21	1614700	511	Heating, Ventilation, and Air Conditioning	In-cell fire	Analysis showed event not to be credible.	
84		1614700	512	Heating, Ventilation, and Air Conditioning	Operator injury from rupture of cell confinement because of ventilation system maloperation.	Design precludes event.	
85	17	1614700	538	Heating, Ventilation, and Air Conditioning	Filter fire	Analysis showed event not to be credible.	
86	53	CCS	1000	Bulk Cold Chemical Storage	Breach of ammonia tank, release of ammonia	Design to prevent tank breach.	Ammonia may be replaced or not needed.

APPENDIX 1A – BNFL INC. OVERALL SAFETY APPROACH

To support the Construction Authorization Request (CAR), BNFL Inc. will submit a Preliminary Safety Analysis Report (PSAR). The PSAR will contain a hazard review based on the Stage B EFDs prepared for the design submitted with the Financial Closure Package. The hazard review will update the information provided in the HAR.

After the submittal of the PSAR, the formal HAZOPs intended to be performed during Part B will be conducted using the Stage D EFDs. These hazard reviews normally are designated HAZOP II in BNFL, plc procedures and denotes a rigorous detailed examination of hazards based on fully developed EFDs.

To support the Operation Authorization Request (OAR), BNFL Inc. will submit the Final Safety Analysis Report (FSAR). The FSAR will contain the hazard review bases for the HAZOPs and the safety basis for the final pre-operational design of the facility.

3.2 STANDARD CONFINEMENT BARRIER APPROACH

To ensure radioactive or hazardous materials do not adversely impact the public or the workers, a series of barriers are provided. These barriers, termed confinement, generally are independent of each other such that internal events that can give rise to the potential for the failure of one barrier will not fail the others. Design features of these barriers ensure that external events (e.g., seismic) that have the potential to fail all barriers, will not have such an effect and at least one barrier survives.

The primary barriers that provide confinement are process vessels, piping, and a dedicated vessel ventilation system (C-5). The vessel and piping are contained within cells. Cell structure and ventilation system (C-5) constitute the second level of confinement. If primary confinement vessels or piping should fail, secondary confinement (i.e., the cell structure has stainless-steel cladding, leak detection, and liquor recovery systems) confine the material in-cell.

Cells where radioactive materials are handled are surrounded by bulk shielding. This provides passive protection to the facility worker against the challenge of excessive dose during facility operations.

A third barrier is provided by the operating corridor outside the cell together with another dedicated ventilation system to prevent radioactive or hazardous material entering operating areas and challenging worker safety. To ensure that radioactive contamination associated with in-cell process operations is suitably confined, conservatively designed ventilation systems provide a continuous, cascade airflow from areas with low potential for radioactivity through to areas of increasing potential. In this way, the potential for any exfiltration of radioactive or hazardous material from cell areas into an operating area is greatly reduced. Ventilation systems exhaust to the facility stack. All effluents are monitored before release. The stack is 88 m high in conformance with WAC 246-247-120 (2.5 times building height).

The three barriers described above ensure that radioactive or hazardous materials will not escape the process into operating areas and give rise to a radiation or a contamination challenge to the facility worker.

Vessels, piping, cell structures, and bulk shielding provide passive protection to the facility worker (as well as to the co-located worker and public). Their safety function will be demonstrated by the application of suitable design standards and regular testing and monitoring. In addition, operating

APPENDIX 1A – BNFL INC. OVERALL SAFETY APPROACH

area radiation monitors, set at a fraction of the allowable limits for normal operation, are installed. The ventilation systems are active systems. To ensure that portions perform safety functions, redundancy of essential components (e.g., fans, status monitoring, electrical power) is provided as appropriate and regular testing and maintenance are conducted.

3.3 USE OF BNFL ENGINEERING DESIGN STANDARDS

The design of BNFL facilities is based on operating and maintenance philosophies that ensure efficient process operation while safely protecting the public, workers, and the environment. These philosophies are based on design methods and features that have evolved with the construction and operation of facilities to ever move stringent workforce public, and environmental protection target at BNFL sites over the last 15 years.

The process follows a logical approach beginning with defining the basis of design and developing the overall process flowsheet system-specific flow diagrams, such as ventilation flow diagrams, if required. The next stage is the utilization of operational and maintenance philosophy documents for each area of the facility. These can be tied together using the overall plant control philosophy document. These documents define the design principles for each area and allow specific equipment selection or design to commence. These are based on existing successful operations of SSCs at Sellafield, and satisfy the BNFL Engineering Design Safety Principles (EDSP). The BNFL EDSPs are similar to the DOE top level safety principles for TWRS. For example, there are direct matches for defense-in-depth, safety quality culture, risk assessment, and the protection against common mode/cause.

The BNFL standard design process completes the safety engineering by the production of discipline-specific Design Justification Reports (DJR). The DJR will substantiate that the design intent has been met and that this has achieved the safety function or classification required with adequate margins of safety.

An example of the BNFL standard “baseline” design approach is the confinement of highly active nitric acid liquors. BNFL would employ primary confinement of a stainless-steel vessel or tank designed and specified in accordance with BNFL’s categorization of vessels standard V001/1 to nuclear chemical standards. Secondary confinement would be provided by a stainless-steel cell liner with the concrete cell structure providing tertiary confinement in addition to radiation protection.

For TWRS C-5 ventilation extract system, the standard BNFL approach, based on AECP 1054 and radiological classification of areas NF 0082/3 has been taken. The system has primary and secondary high-efficiency particulate air filters, and each bank has duty and standby sets. Three 50% rated fans are provided, with 2 duty and 1 standby set with automatic start capability of the standby set.

The TWRS control, electrical, and instrument design basis is defined in R0104. This document defines standards to be applied in the design. For example, NF 0124.1 and .2, *Operational and Engineered Protective Measures*, is identified for use in this instance.

3.4 PROTECTION FOR COMMON MODE/COMMON CAUSE FAILURES

Identification and analysis of hazards for the facility are carried out several times during the design phase. Early hazard studies ensure that safety is incorporated into the design early by identifying

the major hazards. Hazard identification detail is commensurate with the degree of design detail being studied. The study of the conceptual design, the early stage of hazard study, is based on process flow diagrams that indicate the major process vessels and their relationships.

The identification of common mode and common cause failures at the conceptual design stage is limited to the identification of major common cause events with the potential to challenge multiple barriers. Such events include natural phenomena hazards (NPH), loss of offsite power, and fire. Section 3.4.1 describes the approach to these events at this stage of the design.

There are other initiating events that lead to the potential for common cause failures inherent within the process, but a comprehensive identification of all of them at the conceptual design stage is unlikely. The level of detail in the design is not sufficient to fully understand the potential ramifications of the major common cause events. As detailed design information becomes available, the systematic hazard identification studies include guidewords to focus the study team on common mode and common cause failure events, as discussed below.

3.4.1 Part A Common Cause Evaluations

1. NPH (Earthquake, extreme weather)

The design approach to natural phenomena on TWRS-P is to provide a passive design to confine radioactive and hazardous materials under credible NPH conditions. These are defined by reference to the specific design basis events defined in the ISAR and NPH design basis loading provided in the SRD. For example the design basis earthquake (DBE) is taken as 0.24 g with a 2,000-year return period. The TWRS-P approach is to ensure that the design basis event will not result in the release of radioactive or hazardous material such that the public or worker exposure standards are exceeded. The implementation of this approach relies on passive rather than active protection.

The TWRS-P approach is implemented by specifying appropriate seismic design criteria and quality assurance requirements for TWRS-P vessels and piping that contain substantial radioactivity or chemical material inventory. These vessels and piping are protected from common cause effects by specifying suitable seismic Design Criteria (II over I) for any SSCs whose structural failure would likely compromise the primary barrier. As discussed below, loss of power (which would be a likely result of a major earthquake) is not identified as an initiator leading a release of radioactive or chemical material. No other potential common cause effects have been identified at this stage of the design. No further mitigation is necessary because the initiating event (i.e., the earthquake) does not lead to a significant release.

This seismic design approach results in Seismic Category I process vessels and piping. These components are housed in Seismic Category II structures. Process vessels and piping whose failure would lead to unmitigated consequence approaching the public or worker exposure standards are designated Safety Design Class.

As the design evolves, SSCs whose failure could challenge the integrity of the Seismic Category I components also will be designated as Seismic Category II. The iterative hazard analysis process will identify additional common cause failures that might present challenges. These challenges will either be designed out or mitigated.

APPENDIX 1A – BNFL INC. OVERALL SAFETY APPROACH

The hazard evaluation has not yet addressed the potential effect of continued operation of the process pumps following the earthquake in any detail. Preliminary evaluation based only on the capacity of the tankage indicate that this condition would result in minimal leakage. If detailed evaluation determines that this condition results in a significant release, additional protection will be provided. Design options would be considered (e.g., upgrades to the secondary confinement barrier or design provision to trip the pumps).

2. Loss of Offsite Power

The HAR has not identified loss of offsite power as an event leading to a release of radioactive or chemical material. A loss of offsite power would not present a challenge the passive barrier provided by the process vessels and piping and would not present a direct challenge to the barrier comprised of the cell structure and the C-5 extract system.

3. External events (e.g., aircraft crash, missiles)

HAR Sections 2.1.3.2 through 2.1.3.4 indicate that a light aircraft crash into TWRS-P is a credible event. The conceptual approach to this type of hazard is to establish design criteria to prevent significant challenges to the primary confinement barrier. The implementation of this approach will be similar to the NPH design approach illustrated above.

4. Fire

Fire has not been analyzed at this stage of the TWRS-P design. ISAR Section 4.6.5 discusses the approach to fire hazard analysis (FHA) and fire protection design that will be followed in Part B. The results at the initial FHA will be provided in the PSAR. The FSAR will provide an updated FHA.

Common Cause/Common Mode – Part B Detailed Design

With design maturity comes the necessary level of detail required to identify the potential for common cause failures within the process. This is achieved by detailed, systematic, team-based hazard identification studies. The need to protect against common cause events is commensurate with the severity of the hazard that could arise as a result of the occurrence of the common cause failure mode.

The design process for the control of hazards deals with common cause or common mode failure events by specifying protection commensurate with the hazard severity as discussed in Section 4.1. For hazards identified and assessed as having minimal risk, the need for specific protection against common cause events is not necessary because this is at variance with the need to provide a degree of protection against a hazard commensurate with its assessed severity.

Section 3.5 gives an outline of the BNFL standard which shows how the potential for dependent failures is treated in identifying hazard control.

APPENDIX 1A – BNFL INC. OVERALL SAFETY APPROACH

3.5 STRATEGY FOR TREATMENT OF COMMON CAUSE AND COMMON MODE FAILURES IN THE BNFL DESIGN PROCESS

3.5.1 Definitions

Common Cause: When multiple failures result from a single shared cause external to a set of components or system, e.g., external events such as NPH, internal flooding and fire.

Common Mode: When multiple failures occur by the same failure mode within the system, e.g., a set of valves fail to move to the closed position.

These are known generically as dependent failures.

Redundancy: Provision of alternative (identical or diverse) elements or systems so that any one can perform the required function regardless of the state of operation or failure of any other.

Diversity: Dissimilar means of achieving the same objective. It usually refers to the different methods, components, materials etc., in redundant SSCs Important-to-Safety to minimize the probability of simultaneous failure from the same cause.

Independence: For systems to be considered independent, they must not be bound or subject to one another. It is unlikely that separate systems can be totally independent, but the level of independence between separate systems can be increased by e.g., use of different types of equipment.

3.5.2 Summary

Treatment of dependent failure modes is by the provision of protection (control) which has the attributes of redundancy, diversity, or independence. The degree to which these attributes are required will depend on the severity of the hazardous situations being prevented or mitigated.

Basic Principle: There will be demonstrated separation of SSCs for process/facility control and SSCs Important-to-Safety, e.g., where closure of a valve is deemed Important-to-Safety, a separate control valve and safety shut off valve will be provided. Both are required to perform the same function – to isolate line/vessel etc.

3.5.3 Process

The requirement to protect against dependent (i.e., common cause, common mode) failures is proportional to the severity of the hazardous situations which may result from that failure. Therefore, in order to deal with dependent failures the following process takes place:

1. Identification of failure events.
2. Determination of the hazard severity which results from those failures.
3. Determination of the requirement for protection for each initiating event which can lead to the hazard.
4. Determination of the need for protection to be single failure proof.

APPENDIX 1A – BNFL INC. OVERALL SAFETY APPROACH

How this is done is described below.

1. Identification of Failure Events

During Part A, the PHA[2] identified major hazards, each hazard having a limited number of contributory causes. The PHA intent, following the AIChE guidelines[3], is to identify major hazards, the level of design detail precludes the ability to define a comprehensive listing of contributory causes. With the emphasis on the hazard, the PHA studies are able to identify common cause failure events but not necessarily their effects. So, for example, loss of power is identified as an initiator but, due to the limited design detail, its effects on the facility cannot yet be determined.

The use of HAZOP studies in Part B is the method by which dependent failures are identified. Use of a systematic team based review of the detailed design ensures that a comprehensive listing of initiating events against each hazard is generated.

2. Determination of Hazard Severity

Use of standard analysis techniques (consequence determination, frequency assessment) determine the potential severity of a hazard in terms of risk and hence the degree of protection (control) required. In this way the adequacy of protection is tied to how well a risk target is met with respect to margins.

3. Determination of the Requirement for Protection

The BNFL Guide, NF 0124[4] defines how adequate protection is to be provided against identified initiating events, each of which, if allowed to go unchecked, could lead to the hazard. For this to be effective:

- Frequency target for the hazard is defined
- Initiating event frequency is determined
- Hazard severity in terms of consequences is determined

Protection is identified for each initiating event using NF 0124. This engineering standard bins initiating events (which could lead to the hazardous situation) by frequency and hazard severity (consequence). This allows tailoring of the protection requirement for each initiating event to the severity of the hazardous situation.

The Guide, NF 0124 defines the robustness of engineered protection in terms of failure probabilities (probability of failure on demand, pfd); integrity levels for engineered protection are assigned on this basis. These range from level 1 (pfd $<10^{-1}$ to 10^{-2}) to level 4 (pfd $<10^{-4}$ to 10^{-5}). In numerical terms, the guide allows a level of protection to be chosen which, in conjunction with the initiating event frequency, can demonstrate that target frequencies are met.

---

[2] "Process Hazards Analysis", BEL document.

[3] "Guidelines For Hazard Evaluation Procedures", AIChE 1992

[4] NF 0124 entitled "Operational and Engineered Protective Measures" (BNFL April 1997) is a BNFL Engineering Standard which will be adopted into the BNFL Inc. engineering standards for identification of protection requirements.

APPENDIX 1A – BNFL INC. OVERALL SAFETY APPROACH

The robustness of protection is proportional to hazard severity. NF 0124 assigns engineered protection integrity levels (IL) to hazards of defined severity (risk) by means of a matrix.

4. Determination of the need for protection to be single failure proof

To ensure that the potential for dependent failures is identified in proposed protection requirements, NF 0124 makes use of configuration diagrams. Configuration diagrams are a schematic illustration of how protection systems operate to detect and terminate the hazardous situation. They are especially useful for control and instrument systems called out as protection to show the necessary level of redundancy and/or diversity. One diagram supports each fault sequence (the route from the initiating event to the onset of the hazard). Configuration diagrams show the level of independence and acceptable cross connections between different protection systems such that any potential for dependent failures is recognized and so can be eliminated.

The more severe the hazard, the greater is the requirement to prevent its occurrence via common mode failure events. Hence the protection requirements (integrity level) for hazards of moderate to high severity, specify that protection is single failure proof. This means that protection must be vested in at least two independent means of hazard detection, prevention, and termination. This will be redundant or diverse (highest reliability).

The end result is the protection requirements to control hazardous situations are specified for the designer; these take due account of the need to design against dependent failures. In order that the protection design takes account of the potential for dependent failure, there are a number of attributes which the designer needs to consider applying to the engineered protection specification which ensure that its susceptibility to common mode failure is minimized. These attributes include the following:

A. Inherent safety. The elimination of the fault condition for which protective measures (protection, hazard control) would otherwise need to be specified. This is the most effective step to minimize the potential for dependent failure. This is BNFL's preferred approach. This approach takes place during the systematic hazard identification study. If inherent safety can be made part of the design, the relevant hazard study team member is given an action to eliminate the particular hazard.

B. Redundancy and diversity. The need for diversity (provision of dissimilar protection system) is part of the NF 0124 design guide; its requirement is proportional to the assessed hazard severity. A particular application of this is in the basic principle that SSCs for protection are separate from those required for process control.

C. Separation/segregation. This attribute minimizes the potential for common cause failures. This can take the form of physical separation or isolation of systems from each other. For example, it may be prudent to physically separate the two incoming electrical supplies to a C5 fan system to protect against the potential for a fire in one area affecting both supplies.

Other factors which contribute to ensuring that protection is adequately designed to take account of the potential for common mode failure include reliability of essential services, failure state of the facility in the event of loss of service, the need to take account of the operating environment of the engineered protection and adequate operator training.

APPENDIX 1A – BNFL INC. OVERALL SAFETY APPROACH

3.5.4 Conclusion

BNFL has a process by which the potential for dependent failures is addressed. The need to take account of dependent failures is proportional to the hazard severity. An assessment of the potential for dependent failure is carried out at the detailed design stage when a comprehensive listing of initiating events for identified hazards has been made. Protection for each initiating event is identified having first determined the failure logic from the event to the hazard. The reliability of that protection is commensurate with the hazard severity; higher reliability protection is required to be single failure proof. Where inherent safety cannot be provided, the designer takes account of the attributes the protection needs to exhibit in order to be single failure proof. Some of the more important attributes are redundancy/diversity, segregation, and operator training.

APPENDIX 1A – BNFL INC. OVERALL SAFETY APPROACH

4.0 DEFENSE-IN-DEPTH ANALYSIS PROCESS TOPICS

Defense-in-depth includes application of multiple barriers for the protection of hazardous situations and the maintenance of safety margins.

4.1 DEFENSE-IN-DEPTH

This section discusses the BNFL Inc. approach to defense-in-depth and outlines how implementation of this approach will be documented.

4.1.1 Elements of Defense-in-Depth

Multiple layers of protection are applied against hazardous situations. Protection includes engineered features and administrative controls. An engineered feature is either passive or active; passive protection features are inherent features of the design (e.g., shielding) that provide protection without the need for any action. In the selection of controls, preference is given to engineered features over administrative controls. Preference is also given to passive over active engineered features.

Multiple barriers are an aspect of defense-in-depth. The process vessels and connected piping containing the hazardous material and the vessel ventilation system provide the primary barrier against the release of radiological or hazardous material. Secondary confinement is the cell that contains the vessel and connected piping, and the ventilation systems serving the cell. Tertiary confinement, in the form of the operating corridor outside the cell, together with a filtered ventilation system limits the release of the hazardous materials.

Design features that reduce exposure are conservatively assessed to ensure adequate protection against hazardous situations. Design features that offer defense against the potential for exposure include shielded maintenance areas (bulges), ventilation systems providing filtered release, and area radiation and airborne monitoring systems that warn personnel of changing or unsafe conditions.

Training and procedures are administrative controls that serve to reduce the probability of operator error and facilitate prompt and proper operator response to off-normal conditions. This prompt and reliable operator response serves to reduce the challenges to engineered safety features. When off-normal situations occur, the protection against release of radiological and hazardous materials is ensured by activation of protection features that terminate the event.

Emergency preparedness is the final element of the TWRS-P Project approach to defense-in-depth. Emergency preparedness provides assurance that, should a significant radiological and chemical release occur, prompt action can be achieved to limit the exposure to the public and the workers. Emergency preparedness includes emergency plan implementing procedures as administrative controls and instrumentation to detect and monitor the progression of accidents as engineered features.

APPENDIX 1A – BNFL INC. OVERALL SAFETY APPROACH

BNFL applies defense-in-depth by specifying that protection against a hazardous situation is a combination of engineered features and administrative controls providing prevention and mitigation. This means that excessive reliance is not placed on any one system to provide the safe operating environment. Each protection system (i.e., preventative or mitigative) provides the required degree of protection on its own. The BNFL design process bins hazardous situations according to their assessed consequences and frequency, which results in obtaining a hierarchy of hazardous situations according to their severity. Generally, the more severe the hazardous situation, the greater the level of protection that will be specified.

4.1.2 Implementation of Defense-in-Depth

In Part B, defense-in-depth tables will be prepared to identify the control strategies relied on to protect the public and the worker. The defense-in-depth tables (Table 4-1) are developed from the HAZOP and initiator sets determined from qualitative fault trees. Other information used in constructing the defense-in-depth table are the worker safety categories assigned in the process hazard analysis, which includes an updated Hazardous Characteristics Table and an Interaction Matrix. The injury and illness worker safety categories, from AIChE 1992, are shown in Table 4-2 along with project-specific radiation exposure guidelines. Similar tables will be used to document the application of defense-in-depth for public safety. The “public safety category” would relate to radiological and chemical exposure standards provided in ISAR Section 4.6.4.1, “Protection of Public Safety”.

Table 4-1. Defense-in-Depth

PHA Event No.	Accident Description	Worker Safety Category	Initiators	Defense No. 1	Defense No. 2	Defense * No. 3
1						
2						
3						

* Not limited to these levels.

Table 4-2. Worker Safety Categories

Category	Injury or Illness	Exposure (rem)
1	No injury or occupational safety impact	#1
2	Minor injury or moderate occupational illness	1-5
3	Injury or moderate occupational illness	5-25
4	Death or severe occupational illness	>25

APPENDIX 1A – BNFL INC. OVERALL SAFETY APPROACH

A discussion of each initiator, accident, or event and its defenses and common mode failures is provided. Common mode and common cause failures are also considered potential initiating events. An understanding of the initiators is essential to the task of providing passive barriers, prevention and mitigation systems, and an administrative system that protects the worker.

There is no limit to the number of barriers that may be identified nor is there a requirement to demonstrate a minimum number of layers of defense-in-depth. The protection provided for a given hazard is commensurate with industrial practices for relevant types of activity. The presentation will be in a systematic manner (i.e., inner to outer) to clearly identify the layers of defense. This does not imply that the first listed barrier is either the most important or the most reliable.

Facility design germane to defense-in-depth typically includes SSCs that function as the following:

- Barriers to contain uncontrolled hazardous or energy release
- Preventative systems to protect those barriers
- Systems to mitigate uncontrolled hazardous material or energy release on barrier failure
- Interlocks and controls to prevent access to high radiation sources

Administrative controls are linked to the overall safety management programs that directly control operation. Administrative features include the following aspect of operator interfaces:

- Procedural restriction or limits imposed
- Manual monitoring or critical parameters
- Equipment support functions

In addition, as discussed in Section 2.6, BNFL Inc. will perform risk analyses to confirm that facility accident risk goals are met. These risk analyses may show that certain events are significant contributors to the overall accident risk. Additional defense-in-depth items will be specified to reduce that risk. Conversely, if the risk assessment identifies areas of excessive conservation, unnecessary controls may be removed.

4.2 ASSURANCE OF SAFETY MARGIN

The fundamental BNFL approach to establishing a safety margin is preferential selection of passive or inherently reliable means to accomplish safety functions. During the design process, when a potential hazard is identified, the first effort is to design it out of the facility. Removal of a hazardous chemical from the facility is an example of designing out a hazard. If that is not practicable, the next step is to devise prevention or mitigation features that provide protection in the most inherently safe and reliable manner.

Safety margin is designed into the facility through a series of steps as follows:

- Conservative identification of the hazards and hazardous situations. This is achieved, in part, by direction to the process hazards analysis teams that they include hazards and hazardous situations in the records even though the team may believe that the event is highly unlikely or would not have significant consequences (Section 2.3.5 of the TWRS-P PHA procedures previously provided to the RU)
- Conservative analysis of the hazardous situations. This includes, for example, conservative assumptions as to the material at risk, the amount of respirable material released from the

process vessel, the dispersion of the material to the environment, and the uptake of radionuclides by the receptor (see Section 4.6.4 of the ISAR, last paragraph)

- Conservative assessment of the capability of Safety Design Class SSCs to perform their specified safety functions (e.g., assess system flows at less than the design value)
- Conservative selection of design limits from industry consensus codes and standards. These codes and standards provide a margin between the design acceptance limit and the design failure point
- Selection of design and quality assurance requirements applied to increase confidence that the specified safety function will be provided
- Provisions for appropriate inspections, tests, and surveillance during the component or system operating life to ensure allowances for deterioration and aging are adequate (allowance for wall thickness degradation).

Technical safety requirements provide assurance of the continued operability of active Safety Design Class features by the implementation of testing and surveillance requirements.

APPENDIX 1A – BNFL INC. OVERALL SAFETY APPROACH

5.0 SAFETY DESIGN CLASSIFICATION TOPICS

5.1 RELIANCE ON DOSE MODELS

The overwhelming majority of the safety items in the TWRS-P design are not based on dose models but on proven, successful experience controlling similar hazards in facilities located both in the UK and the United States. This includes those safety items identified through the following:

- Application of the standard confinement barrier approach (Section 3.2)
- Application of the BNFL engineering standards (Section 3.3)
- Specification of event-specific controls (Section 2.1)
- Defense-in-depth evaluation process (Sections 2.2 and 4.1)
- Specification of Safety Design Class SSCs that protect the facility worker from potentially severe events (Section 2.3)

Two of the BNFL safety processes – accident risk evaluation and, in part, safety design classification – do rely on dose models to identify safety features of the design. However, in these cases, the use of dose models is necessary to demonstrate compliance with accident risk goals and accident consequence standards, respectively. Without this demonstration of compliance, the conformance of the BNFL design to the associated top-level standards of DOE/RL-96-0006 could not be established.

The above discussion demonstrates that (1) BNFL's approach to safety utilizes dose models appropriately, and (2) the BNFL approach is not overly reliant on those models for the identification of safety items.

5.2 APPROACH TO PUBLIC AND WORKER PROTECTION

BNFL Inc.'s approach provides an adequate level of accident protection for both the public and workers. This is achieved, in part, by the designation of Safety Design Class SSCs. These SSCs, which ensure that accident exposure standards are not exceeded, are assigned the highest levels of design, quality assurance, and operational requirements.

It should be noted that the same requirements are applied to a Safety Design Class SSC regardless of whether it is associated with worker protection or public protection. This would include, as appropriate, the capability of accident prevention/mitigation features to withstand credible single failures.

APPENDIX 1A – BNFL INC. OVERALL SAFETY APPROACH

6.0 IDENTIFICATION OF IMPORTANT-TO-SAFETY ITEMS

SSCs defined as Important-to-Safety for the TWRS-P Facility include the following.

1) SSCs needed to prevent or mitigate accidents that could exceed public or worker radiological and chemical exposure standards and SSCs needed to prevent criticality. This set of SSCs includes front line and support systems needed to meet these exposure standards. This set of Important-to-Safety SSCs are further designated as Safety Design Class.
2) SSCs needed to achieve compliance with the radiological or chemical exposure standards for the public and workers during normal operation; and SSCs that place frequent demands on, or adversely affect the function of, Safety Design Class SSCs if they fail or malfunction.

The processes for identifying the SSCs for each of the two groups of SSCs Important-to-Safety and the requirements assigned to each of the two groups are discussed below.

The first group of SSCs classified as Important-to-Safety (i.e., those needed for accident prevention or mitigation or criticality prevention) are identified by the safety classification process described in ISMP Section 1.3.10, “Classification of Structures, Systems, and Components” but with the change that this set of SSCs is no longer divided into Design Class I and II. In response to RU concerns, the classification of SSCs as DC I and DC II is replaced by a classification process that identifies SSCs as “Safety Design Class” if the SSC is needed to protect either the public or workers from the consequences of accidents such that exposure standards are not exceeded.

The second group of SSCs classified as Important-to-Safety (i.e., those that could challenge safety functions or are needed to limit releases during normal operation) are identified in several ways including: (1) SSCs identified as significant contributors to safety by the risk analyses that confirm the facility accident risk goals are met, (2) implementation of defense-in-depth as discussed in Section 4.0 of this appendix, (3) performance of HAZOP Analysis, (4) design review of those systems that limit worker or public exposure to radionuclides and chemicals, and (5) SSCs whose failure could prevent Safety Design Class SSCs from performing their safety function (e.g., seismic II/I items).

Important-to-safety SSCs needed to prevent or mitigate accidents that could exceed public or worker exposure standards (i.e., Safety Design Class SSCs) are identified in ISAR Section 4.8.1.1, “Design of Class I Engineered Features”, and listed in ISAR Tables 4-46 and 4-47 (currently identified as DC I and DC II in the ISAR). Criticality has been determined as an incredible event at this stage of design of the TWRS-P Facility and therefore criticality prevention is not dependent on engineered features.

As stated in Section 4.8, of the ISAR, “The selection of engineered and administrative controls is based on the conceptual design of the facility. Additional and even some different features may be identified during Part B.” The more complete group of Important-to-Safety SSCs will be identified in Part B and provided in the Preliminary Safety Analysis Report as part of the Construction Authorization Request. This group may include SSCs listed in the fault schedules of the Hazards Analysis Report as “safeguards” if there is deemed to be a significant contribution to safety or risk reduction provided by the safeguard.

APPENDIX 1A – BNFL INC. OVERALL SAFETY APPROACH

When an SSC is designated as Safety Design Class (i.e., needed to meet the worker or the public radiological or chemical exposure standards or criticality prevention), it is provided the following attributes:

1. Quality Level 1 (QL-1) is applied to the SSC. Section 1.3.11, "Quality Levels" and Table 1-4 of the ISMP describe the requirements associated with QL-1.
2. For active systems and components, the safety function is preserved by application of defense-in-depth such that the failure of an active system or component will not result in exceeding a public or worker accident exposure standard. For a mitigating feature, this means that, given that the accident has occurred, the consequence of the accident will not result in exceeding a public or worker exposure standard. For a preventative feature, this means that the failure of the system or component will not allow the accident to occur and progress such that a public or worker accident exposure standard is exceeded. This requirement may be achieved by designing the Safety Design Class system or component to withstand a single active failure or by designating two separate and independent Safety Design Class systems or components.
3. The SSC is designed to withstand the effects of natural phenomena such that it can perform any safety functions required as a result of a natural phenomena event. For example, if an earthquake can produce exposures to the public in excess of standards, the Safety Design Class SSC that prevents or mitigates the exposures would be designed to be DBE-resistant. It should be noted, however, that DBE-resistance is not automatically applied to Safety Design Class SSCs. It is only applied when the earthquake is the initiating event, or when the earthquake could cause the initiating event. This design philosophy is also used for the loads imposed by other severe natural phenomena such as high winds or floods.
4. General design requirements are applied equivalent to those invoked in Section 4 of the SRD for Design Class I engineered features (in Part B, reference in the SRD to Design Class I will be replaced with reference to Safety Design Class). See SRD Safety Criterion 4.1-5 as an example.
5. Specific design requirements based on the type of component are applied as invoked in SRD Chapter 4.0. For example, SRD Safety Criterion 4.4-5 provides requirements associated with Safety Design Class (previously DC I) air treatment systems.
6. Other design requirements may be applied based on the specific safety function to be performed by the Safety Design Class SSC. This specific safety function is determined from the accident analysis that identified the need for prevention or mitigation by Safety Design Class SSCs.
7. Operational requirements (e.g., periodic testing and preventative maintenance) are applied to Safety Design Class SSCs through the application of Technical Safety Requirements (discussed in IMP Section 4.2.3.4, "Technical Safety Requirements and Licensee Controlled Requirements"). In response to RU concerns, when Technical Safety Requirements are required to ensure system operability, they are applied to Safety Design Class SSCs regardless of whether they are needed for worker or public protection.

When a SSC is classified as Important-to-Safety but is not needed to meet the worker or public exposure standards (i.e., those that could challenge safety functions or are needed to limit releases during normal operation) it is has the following attributes.

APPENDIX 1A – BNFL INC. OVERALL SAFETY APPROACH

1. Quality Level 2 (QL-2) is applied to the SSC. ISMP Section 1.3.11 and Table 1-4 describe the requirements associated with QL-2.
2. General and specific design requirements are applied equivalent to those invoked in SRD Section 4 for DC II engineered features (in Part B, reference in the SRD to DC II will be to reference this set of Important-to-Safety SSCs).
3. The SSC is designed to withstand the effects of natural phenomena such that it can perform its safety functions required as a result of a natural phenomena event. If an earthquake can produce exposures to the public in excess of standards, the Safety Design Class SSC that prevents or mitigates the exposures would be designed DBE-resistant as discussed above. The same NPH loads are also applied to an Important-to-Safety item that is not designated as Safety Design Class if failure of the item could prevent the Safety Design Class SSC from performing its safety function required as a result of the DBE. It should be noted, however, that DBE resistance is not automatically applied to this set of Important-to-Safety SSCs. It is only applied when the earthquake is the initiating event, or when the earthquake could cause the initiating event. This design philosophy is also used for the loads imposed by other severe natural phenomena such as high winds or floods.
4. Other design requirements may again be applied based on the specific safety function to be performed by the SSC. This specific safety function is determined from the process hazards, risk analysis, defense-in-depth evaluation, and the evaluation of normal releases that identified the need for the SSCs.

APPENDIX 1A – BNFL INC. OVERALL SAFETY APPROACH

7.0 QUALITY LEVELS FOR ITEMS, SYSTEMS, STRUCTURES, AND COMPONENTS

Safety Design Class SSCs are specified to ensure that the consequences of accidents do not exceed public or worker accident exposure standards. Quality Level 1 (QL-1) requirements are applied to a Safety Design Class SSC to provide added assurance that it can perform its safety function.

When an SSC is designated as Important-to-Safety (but not as Safety Design Class), Quality Level 2 (QL-2) requirements are applied to provide added assurance that it can perform its safety function.

Quality Level 3 (QL-3) requirements are applied to other SSCs as appropriate to their function.

Table 7-1 shows the quality assurance program requirements associated with QL-1, QL-2, and QL-3.

Table 7-1. Application of Quality Assurance Program Requirements for QL-1, QL-2, and QL-3 Structures, Systems, and Components

QAP Requirement	QL-1	QL-2	QL-3	Remarks
1. Program				
• A written Quality Assurance Program (QAP) is developed, implemented, and maintained.	X	X	Xa	A QAP describing selected criteria (as applicable) of 10 CFR 830.120 or NQA-1 is acceptable for QL-3.
• The QAP describes the organizational structure, functional responsibilities, level of authority, and interfaces for those managing, performing, and assessing the work.	X	X		
• The QAP describes management processes, including planning, scheduling, and resource consideration.	X	X		
2. Personnel Training and Qualification				
• Qualification of personnel: policies and procedures that describe personnel selection requirements are established for each position.	X	X	Xa	Commercial fraction for QL-3.
• Training provides knowledge of the correct processes and methods to accomplish assigned tasks.	X	X		

APPENDIX 1A – BNFL INC. OVERALL SAFETY APPROACH

Table 7-1. Application of Quality Assurance Program Requirements for QL-1, QL-2, and QL-3 Structures, Systems, and Components

QAP Requirement	QL-1	QL-2	QL-3	Remarks
• Training goals, lesson plans, and other training materials are developed, reviewed by subject matter experts, and approved by management.	X	X		
• Training effectiveness is monitored. Worker performance is evaluated to ensure that the training program conveys all required knowledge and skills.	X	X		
3. Quality Improvement				
• Process to detect and prevent quality problems is established and implemented.	X	X	Xa	Commercial fraction for QL-3.
• Items, services, and processes that do not meet established requirements are identified, controlled, and corrected according to the importance of the problem and the work affected.	X	X	Xa	Commercial fraction for QL-3.
• Correction includes identifying the causes of problems and working to prevent recurrence.	X	X	Xa	Element optional for QL-3
• Item characteristics, process implementation, and other quality-related information are reviewed and the data analyzed to identify items, services, and processes needing improvement.	X	X		
4. Documents and Records				
• Documents are prepared, reviewed, approved, issued, used, and revised to prescribe processes, specify requirements, or establish design.	X	X	Xa	Element optional for QL-3
• Records are specified, prepared, reviewed, approved, and maintained.	X	X	Xa	Element optional for QL-3
5. Work Processes				

APPENDIX 1A – BNFL INC. OVERALL SAFETY APPROACH

Table 7-1. Application of Quality Assurance Program Requirements for QL-1, QL-2, and QL-3 Structures, Systems, and Components

QAP Requirement	QL-1	QL-2	QL-3	Remarks
• Work is performed to established technical standards and administrative controls using approved instructions, procedures, or other appropriate means.	X	X	Xa	Commercial practices for QL-3
• Items are identified and controlled to ensure their proper use.	X	X	Xa	Commercial practices for QL-3
• Items are maintained to prevent their damage, loss, or deterioration.	X	X	Xa	Commercial practices for QL-3
• Equipment used for process monitoring or data collection is calibrated and maintained.	X	X	Xa	Element optional for QL-3
6. Design				
• Design inputs are technically correct and complete. These inputs may include such information as design basis, health and safety considerations, performance parameters, codes and standards requirements, and reliability requirements.	X	X	Xa	Element optional for QL-3
• Technical design interfaces are identified in the input documents and methods are established for their control.	X	X		Element not required for QL-3
• The design process translates design input into design output documents that are technically correct and meet the end user's requirements.	X	X	Xa	Commercial practices for QL-3
• Aspects critical to the safety or reliability of the designed system, structure, or component are identified during the design phase.	X	X		Element not required for QL-3
• Computer software verification and validation.	X	X		Element not required for QL-3

APPENDIX 1A – BNFL INC. OVERALL SAFETY APPROACH

Table 7-1. Application of Quality Assurance Program Requirements for QL-1, QL-2, and QL-3 Structures, Systems, and Components

QAP Requirement	QL-1	QL-2	QL-3	Remarks
• The completed design is recorded in design output documents such as: drawings, specifications, test/inspection plans, maintenance requirements, and reports.	X	X	Xa	QL-3: drawings, specifications, calculations only
• Design verification is a formal documented process to establish that the resulting SSC will be fit for the intended use. Design verification methods include, but are not limited to, technical reviews, peer reviews, alternate calculations, and qualification testing.	X	X		Element not required for QL-3
• The adequacy of design products is verified or validated by an individual or groups other than those who performed the work.	X	Xa		Element not required for QL-3
• Design changes, including field changes and nonconforming items dispositioned “use-as-is” or “repair”, are controlled by measures commensurate with those applied to the original design.	X	X	Xa	Commercial practices for QL-3
• Temporary modifications receive the same levels of control as the designs of permanent modifications.	X	X		Element not required for QL-3
7. Procurement				
• Prospective suppliers are evaluated and selected on the basis of specified criteria.	X	X		Element not required for QL-3.
• Procurement documents clearly state test/inspection requirements and acceptance criteria for purchased items and service.	X	X	Xa	Commercial practices for QL-3
• Supplier monitoring.	X	Xa		Element not required for QL-3
• Receipt inspection.	X	X	X	
• Reporting nonconformances.	X	X	X	

APPENDIX 1A – BNFL INC. OVERALL SAFETY APPROACH

Table 7-1. Application of Quality Assurance Program Requirements for QL-1, QL-2, and QL-3 Structures, Systems, and Components

QAP Requirement	QL-1	QL-2	QL-3	Remarks
• Product documentation: Supplier-generated documents that are important to the product quality are accepted through the procurement system and controlled; these documents may include certificates of conformance, drawings, analysis, test reports, maintenance data, nonconformances, corrective actions, approved changes, waivers, and deviations.	X	X	X	
8. Inspection and Acceptance Testing				
• Inspection and testing of specified items, services, and processes is conducted using established acceptance and performance criteria.	X	X	Xa	Commercial practices for QL-3
• Equipment used for inspections and testing is calibrated and maintained.	X	X	Xa	Commercial practices for QL-3
9. Management Assessment				
C Managers assess their management processes. Planned and periodic management assessments are established and implemented. Problems that hinder the organization from achieving its objectives are identified and corrected.	X	X	Xa	Element optional for QL-3
10. Independent Assessment				
• Independent assessments are planned to measure item and service quality.	X	X		Element optional for QL-3
• The group performing independent assessment has sufficient authority and freedom from the line organization to carry out its responsibilities.	X	X		

APPENDIX 1A – BNFL INC. OVERALL SAFETY APPROACH

Table 7-1. Application of Quality Assurance Program Requirements for QL-1, QL-2, and QL-3 Structures, Systems, and Components

QAP Requirement	QL-1	QL-2	QL-3	Remarks
• Persons conducting independent assessments are technically qualified and knowledgeable in the areas assessed.	X	X		

X = Full application of the QAP requirement

Xa = Graded application of QAP requirements

Source = Initial Safety Analysis Report, BNFL-5193-ISAR-01, Rev. 0.

APPENDIX 1A – BNFL INC. OVERALL SAFETY APPROACH

8.0 TWRS EXAMPLE OF OVERALL PROCESS – HLW RECEIPT TANKS

A process has been described that shows how adequate safety of BNFL designs is developed. Safety by design is developed from the process that involves: (1) hazard identification and control that specifies the required protection; (2) defense-in-depth; (3) the identification of Design Class protection.

To show how this process is applied to the TWRS-P Facility, a worked example using a HLW receipt tank is provided. The detailed design information on vessel instrumentation (e.g., sequence and interlocks, field values) and process logic (e.g., sequence of HLW import, operation of the vessels, sampling) is a Part B activity; protection related to these activities is still to be specified.

8.1 HAZARD IDENTIFICATION AND CONTROL

Our process for ensuring safety is similar to the DOE/RL 96-0004 requirements, where hazard control is the result of identified hazards based on the work to be performed. In this case, the work requirement is to process Envelope D waste from Tank Farm tanks AZ101/102. To achieve this, the material is piped from these vessels via a dedicated valve box to receipt vessels under BNFL control, located at the north end of the TWRS-P pretreatment building. A description of this aspect of the facility process is given in the ISAR Section 4.3.1.1. Data are available from mass balance information, material composition, process flow diagrams, and schematics in addition to the process description.

Based on the radiological characteristics of Envelope D material, the design of these vessels follows BNFL practice for the design of vessels containing radioactive material. The material is contained within vessels constructed of material that will last the design life of the facility and withstand the physical properties of the process liquid. These factors, among others, are considered in the BNFL Vessel Design Guide, which allows the designer to specify the characteristics of the vessels. The TWRS-P vessel data sheet developed from the design guide specifies ASME VIII for the basic design code with initial selection of materials of construction as 316L SS. Surrounding the vessels is a cell lined with material that will resist corrosion by the process liquid. The cell has liquid detection, collection, and treatment facilities. The cell attributes are specified in the NF 82 design guide series, “Radiological Classification of Areas”. Both cell and vessels are served by a ventilation system that draws air from operating areas through the cell and vessels and exhausts it via filters and a stack to the outside. Details of the ventilation system are contained in the TWRS-P ventilation philosophy document. The purpose of the filters and stack is to reduce the impact of the aerial emissions to a low level.

APPENDIX 1A – BNFL INC. OVERALL SAFETY APPROACH

The data available on these vessels (mass balance, material compositions, vessel layouts, and function within the pretreatment process as specified on the appropriate process flow diagram) are the basis for the Process Hazard Analysis (PHA) of this part of the process. The guide words applied by the team focus on the hazard potential of the receipt of Envelope D material into the pretreatment area. Identification of sufficient initiating events to establish the credibility of the major hazards is the major activity of the team. This activity is consistent with the AIChE guidelines for a hazard identification exercise on the level of design detail available for a conceptual design. In considering each of the major hazards, the team made a qualitative judgement as to whether or not they could be designed out and therefore be removed. In this particular area, the potential for explosion due to a buildup of radiolytic hydrogen was considered unacceptable. Design development of the ventilation system is intended to eliminate the potential for a significant buildup of radiolytic hydrogen in a credible time period. This judgement was based on the perceived severity of the hazards and the mitigation offered by the design. If further, more detailed assessment of a hazard indicated that it would be unacceptable, a request would be made to design it out.

The PHA identified the hazards together with their control associated with the receipt of Envelope D material into the HLW receipt vessels, V4101A-C. These are listed in Table 8-1.

Table 8-1. Hazards and Their Control for the HLW Receipt Vessels, V4101A-C

Hazard/Initiating Events	Protection
Catastrophic failure of vessels due to a seismic event	Primary confinement
Corrosion of vessels and pipework	Materials of construction, testing, monitoring
Potential for criticality from out-of-specification feed Not considered credible	Not needed
Activity accumulation within vessels (chronic build up of solids)	Wash rings, water flush
Activity breakthrough to lower activity areas leading to worker dose	Shielding, radiation monitoring, washdown, maintenance procedures
In-cell load drop (crane failure)	Minimize lift height load cells interlocks
Cell pressurization event	Ventilation system, limited air flow/pressure
Fire/explosion	Fire loading, limited potential – long time to build up flammable concentrations of hydrogen, ventilation system
Loss of services (air water power)	Back up supplies
In-cell process liquid leak	In-cell cladding, liquid detection, collection, and treatment
Activity challenge to ventilation system	Temperature and level indications

APPENDIX 1A – BNFL INC. OVERALL SAFETY APPROACH

8.2 DEFENSE-IN-DEPTH EVALUATION

Table 8-1 identifies the controls that may be applied to the identified hazards. At this stage, this is a qualitative evaluation based on concept design detail. Only a few of the hazards identified had hazard severities of 3 and 4 (unmitigated consequences to facility workers, co-located workers, or public). These are as follows:

- Catastrophic vessel failure due to the seismic event
- Activity breakthrough to lower activity areas
- Fire and explosion
- Activity challenge to ventilation system

These are considered, at this stage, to be the severe hazards present in this area of the facility. At this stage, as indicated, only a limited number of initiating events (causes) for each hazard has been identified. Consequently, only a limited specification of protection has been postulated. This may be sufficient for the purposes of the Part A requirements – to determine whether or not the design embodies safety, but it lacks the detail to make a defense-in-depth determination.

The Part B hazard studies to be performed on the detailed design will result in an exhaustive list of initiating events (causes) against each of the identified hazards. The hazard severity will determine the protection requirements against each of the initiating events. A BNFL Design Guide, NF 0124, outlines the process by which this is achieved. So, for example, from the list of severe hazards above for the HLW receipt vessels, the build up of radiolytic hydrogen in vessel ullages to flammable concentrations is one initiating event for fire and explosion. Protection offered includes a vessel ventilation system design that ensures that the vessel ullage will not see a flammable gas concentration in a credible time period under quiescent conditions, no source of ignition, and ventilation system with redundant fan systems. Any one of these protection systems ensures that the hazard – fire and explosion – cannot occur from the presence of radiolytic hydrogen. In this case, no single protection system is relied on for safety, there are several; this is the application of defense-in-depth.

8.3 IDENTIFICATION OF SAFETY DESIGN CLASS SSCs

Having identified potential hazard controls (Part A) and evaluated conformance with defense-in-depth (Part B activity), the accident analysis determines if public, co-located worker or facility worker exposure standards are challenged. For the HLW receipt vessels, only the catastrophic failure of the vessels due to the seismic event has the potential to challenge, in this case, exposure standards for the public. Therefore, the elements of protection offered are designated Safety Design Class.

APPENDIX 1A – BNFL INC. OVERALL SAFETY APPROACH

As indicated in Section 3.4, the approach to protection against the design basis earthquake (DBE) is to ensure that one level of engineered passive protection can be demonstrated to survive the event intact. For the HLW receipt vessels, the primary confinement, the vessels, are designated Safety Design Class. Selection of the primary confinement as Safety Design Class demonstrates a robust level of control, the liquid is confined at source. The defined safety function of the Safety Design Class vessels is to confine the radioactive liquid in the vessel with no leakage to cell. Designation of the vessel as Safety Design Class demonstrates an additional assurance of safety. The design standards for SSCs designated Safety Design Class are found in the SRD. Because the ASME VIII design code has been chosen, which is more restrictive than the API 620/650 codes, the codes and standards requirement for Safety Design Class vessel has been satisfied. The safety function of this vessel will be demonstrated in a design justification report, which will support the PSAR.

8.4 CONFORMANCE WITH THE IMPORTANCE TO SAFETY CONCEPT

As a result of the design process for the HLW receipt vessels, hazards have been identified and their controls indicated. Because the DBE has the potential to challenge public exposure standards, a specific part of that control strategy, the vessels, has been designated Safety Design Class. By definition, therefore, the vessels are Important-to-Safety. In conformance to the definition of Important-to-Safety contained in the DOE-RL documents, the other significant contributors to overall safety can (and will) be defined when further, more detailed, hazard studies take place in Part B.

8.5 INFORMATION THAT THE RISK FROM ACCIDENTS IS ACCEPTABLE

At this stage, it is not possible to decide if the controls indicated against the identified hazards ensure that the risk from the operation of the HLW receipt vessels is acceptable. This can be ascertained only after hazard controls have been completely identified after the detailed determination of initiating events or hazard causes.

APPENDIX 1A – BNFL INC. OVERALL SAFETY APPROACH

9.0 REFERENCES

AIChE, 1992, *Guidelines for Hazard Evaluation Procedures, Second Edition with Worked Examples*, American Institute of Chemical Engineers, New York, New York.